CME Group | Advisory Notice

TO: CME Secure SFTP Users

Advisory Number 16-071

FROM: CME Clearing

DATE: February 11, 2016

SUBJECT: **CME Ciphers and MACs SFTP Changes, April 9, 2016**

To enhance security of customers' connectivity to CME Secure SFTP, effective Saturday April 9, 2016, CME will update our supported list of ciphers and MACs. This change will impact connectivity to CME SFTP.

Following the update, firms must use at least one of the Ciphers and one of the MAC's listed below:

Supported Cipher algorithms:

- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc
- aes192-cbc
- aes128-cbc

Supported MAC algorithms:

- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1

Failing to do so will impact firms' ability to access CME SFTP.

Firms can test this enhancement in the Testing SFTP site starting on Monday, February 29, 2016. Below are the site information and testing procedure:

- Web based site address: **sftpcert.cmegroup.com**
- Will accept the same credentials currently used for Production SFTP site.
- Firms can send a test file into the Incoming folder
- Or Download test file "**CME.Cipher.Test.xml**" from the Outgoing folder.

Finally, we will offer our customers the opportunity to test their connectivity into production SFTP on Saturday, April 9, 2016 following the implementation. For more information please contact CME Clearing at (312) 207-2525 ccs@cmegroup.com.

Thank you
CME Clearing